



$$\left\{ \begin{array}{l}
 \text{IS} - \left\{ \begin{array}{l}
 X \xrightarrow{g} n \quad X \xrightarrow{g} n \quad X = g^x \bmod n \\
 Y = g^y \bmod n \quad Y \xrightarrow{\quad} Y \\
 K = X^y \bmod n \quad K = Y^x \bmod n
 \end{array} \right.
 \end{array} \right.$$

$$\left\{ \begin{array}{l}
 \text{PS} - \left\{ \begin{array}{l}
 PD = \text{dec}(K; PD_K) \quad PD_K \quad PD = \text{dec}(KM; PD_{KM}) \\
 PD_K = \text{enc}(K; PD) \quad PD_K \quad PD_{KM}
 \end{array} \right.
 \end{array} \right.$$

Fig.